© FEB 2026 | IRE Journals | Volume 9 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I8-1714299

Design And Implementation of An Intelligent Erp System Integrated with A Role-Based Access Control (RBAC) Mechanism

CHIDI-EZEH SYLVIA CHINASA[1], K. M OKORIE[2]
[1, 2]*Enugu State University of Science and Technology*

Abstract- ***Enterprise Resource Planning (ERP) systems play a critical role in modern organisations by integrating business processes and enabling data-driven decision-making. However, despite advances in intelligent ERP platforms, many systems most especially within small and Medium-Sized Enterprises (SMEs) and developing economies which continues to suffer from weak access control mechanisms, exposing sensitive organisational data to insider threats and unauthorised access. This study proposes the design and implementation of an intelligent ERP system integrated with a Role-Based Access Control (RBAC) mechanism to enhance data security, operational efficiency, and administrative control. A hybrid development methodology combining Agile practices and the Spiral Model was adopted to ensure iterative refinement, stakeholder involvement, and systematic risk management throughout the system development lifecycle. The proposed RBAC framework adopted in the study defines hierarchical access levels based on organisational roles therefore enabling controlled access to ERP modules such as finance, human resources, inventory and project management. Furthermore, a Rule-Based algorithmic model was developed to govern user authentication, role identification, access evaluation, and continuous security monitoring. The system was implemented as a web-based application and evaluated through functional testing and user interaction scenarios. Results from the implementation demonstrate that the integration of RBAC effectively restricts unauthorised access, improves accountability through activity logging, and enhances overall system usability. Then the study concludes that embedding intelligent access control mechanisms into ERP systems significantly strengthens data protection and supports secure, scalable enterprise operations. The proposed framework offers a practical and adaptable solution for organisations seeking to improve ERP security and governance.***

Index Terms- ***Enterprise Resource Planning (ERP); Role-Based Access Control (RBAC); Intelligent Systems; Access Control Security; Information Systems Security***

I. INTRODUCTION

Businesses are being impacted by a number of sociological and technical changes in today's dynamic environment. Automation, an abundance of data, and intelligent technologies that use data to learn from and respond to surroundings are some of the trends (Rashid and Kausik, 2024). Businesses utilise Information Systems (IS) to handle important data, and having timely access to the appropriate information helps businesses stay competitive (Taherdoost, 2022). In order to improve competitiveness and sustainability, businesses need to be able to detect their surroundings, respond intelligently based on the data collected, and make choices more quickly and effectively. Enterprise Resource Planning (ERP) solutions are utilised by several organisations to connect data, applications, and business processes from different departments and sources (William and Tjhin, 2021).

ERP systems are all-inclusive, integrated platforms that may be used on- or off-site to handle all aspects of a distribution or product-based business. ERP systems serve all aspects of financial operations, such as production, force chain operations, and treasuries, much like main account functions (Uemerson, 2020). ERP systems provide transparency across the whole business process by managing all aspects of the company's finances, logistics, and products equally. Access points for different departments are provided by these networked systems, which act as the central hub for end-to-end workflow and data in an organisation (Gessa et al., 2023).

ERP systems are much more than just back-office transactional systems in today's businesses; they are fundamental engines that generate and use vast amounts of data (Accenture, 2020). Nevertheless,

they are also completely interconnected and serve as the foundation for digital transformation. According to recent market research, the ERP market has enormous potential and is predicted to more than double in size, reaching 86.303 million USD by 2027 from its 2019 valuation of 39.340 million USD (Gaikwad and Rachita, 2021). ERPs evolved from a basic inventory management system in the 1960s to a digital supporting system for nearly all organisational operations due to organisational and technical potential (Goldston, 2020; Gessa et al., 2023). Future ERPs will be significantly impacted by ongoing advancements and fresh prospects. ERP vendors and consumers have difficulties in implementing these advancements, which is a continuous process (Brodzik et al., 2020).

Lack of organised and enforced access restrictions is one of the main weaknesses in many ERP systems, allowing organisations to improperly manage what people may access or do with them. According to Clark (2022), Yahoo sued Qian Sang, a former senior researcher, on charges of stealing a significant quantity of private data. Sang, who oversaw a key group in Yahoo's advertising operation, is accused of downloading up to 570,000 pages of private information, including strategy papers, algorithms, and proprietary source code. Block Inc.'s financial services platform Cash App was the focus of a data security issue in December 2021 when a former employee took 8.2 million users' identities and broking investment details without authorisation (Paganini, 2022). In order to control how information and data are used within the organisation, every organisation must adopt a digitalised access control approach, even though traditional methods like employee monitoring can help protect the organisation from problems like these with ERP (Marquis, 2024).

These incidents demonstrate the need for more thorough approaches, such as Role-Based Access Control (RBAC), which provides a stronger system protection. Together, these occurrences highlight the need for research on RBAC's potential to strengthen database security against insider attacks. They draw attention to serious flaws in the way security is currently handled, such as insufficient user access checks, poor termination procedures, and a lack of proactive monitoring for questionable activity. However, issues with precise job definition, dynamic access requirements, and the changing nature of insider threats impede RBAC's effectiveness in practical implementations (Malik et al., 2020). Organisations must include the RBAC approach in order to maximise their resource utilisation and respond more quickly to shifting operational needs in light of the increasing need for more intelligent and secure ERP systems.

II. METHODOLOGY

The methodology adopted for the development of the intelligent ERP system is a hybrid approach that integrates the Agile methodology with the Spiral Model. This combination leverages the iterative, customer-focused nature of Agile with the risk-driven, evolutionary development framework of the spiral model, ensuring both adaptability and robustness in system development. The Agile methodology was employed to ensure continuous interaction with stakeholders, frequent delivery of functional modules and responsiveness to evolving user requirements. Through iterative sprints, the system was broken down into manageable components, allowing for rapid prototyping, testing and refinement based on user feedbacks. This ensured the system’s alignment with organizational workflows and real-time data requirements.

Simultaneously, the Spiral Model provided a structured framework to address potential risks at every development phase. Each iteration of the spiral involved four key stages: planning, risk analysis, engineering and evaluation. This model was particularly valuable in managing the integration of intelligent features such as machine learning-based decision support and role-based access control mechanisms by systematically identifying and mitigating technical and security-related risks early in the development life-cycle. The combination of these two methodologies facilitated a flexible yet controlled development environment. Agile ensured that the system remained user-centric and adaptable, while Spiral Model provided a rigorous approach to risk management, scalability and system validation. Together, they enabled the successful development of

© FEB 2026 | IRE Journals | Volume 9 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I8-1714299

a secure, intelligent ERP system tailored to meet both operational and strategic needs of the enterprise.

III. MODELLING OF THE RBAC BASED ERP MODULE

This section illustrates how the data collected was used to assign access level to the resource persons in the organization according to their roles. The assignment of the access levels is in line with the RBAC principle which gives the highest level of access (4 in this case) to the overall personnels in the organization to oversee the management of other activity records, while the least level has access level of 1 which is usually the general public users of the system, thereby improving the security and integrity of organization's data. Table 4.9 presents the access level assignments administered to the officers according to their roles in the organization.

Table 1: RBAC Access Level Assignment

Data Category	Example Entries	Access	Access Level
User and Access Data	Login records, roles, permissions	Admin Only	4
Financial Data	Budgets, payroll, invoices	Restricted (Admin)	4
HR Data	Employee records, leave reports	Restricted (Manager/Admin)	4/3
Project and Task Data	Task assignments, schedules, KPIs	Shared (Managers and staff)	3/2
Inventory Data	Stock levels, procurement history	Shared (Admin)	4
Communication Logs	Memos, meeting notes, announcements	Public	4,3,2,1
System Logs	Error logs, backups, system settings	Admin Only	4
Security Logs	Login attempts, encryption reports	Admin Only	4
Customer Data	Contact details, support tickets, billing	Restricted (Admin/Manager)	3,4
Document Management	Files, templates, manuals	Public	4,3,2,1

According to Table 1, the various activities performed in the organization and the data representing them are clearly presented and the access levels of the personnel officers are assigned. This is done in order to have a clear control of the roles that have access to certain levels of data and maintain the security and integrity of the data being utilized.

3.1 System Algorithm

The proposed intelligent system integrates an ERP environment with RBAC to ensure secure, modular and manageable access to sensitive business operations or data for dedicated organizations.

Algorithm 1 presents a simplified workflow and logic for the operations of the proposed ERP system.

Algorithm 1: Intelligent ERP

1 Start System
2 User Authentication
    Prompt for Username and Password
    Validate credentials against the Users database
    If authentication fails:
        Display "Access Denied"
        Log attempt and terminate session
    Else:
        Proceed to role identification
2 Role Identification #Fetch user login data (Role and Permission Level)
    Retrieve user's role(s) from UserRole design table in the Database
    Load associated permissions from RolePermission table #Acquire permission level
3 Access Request Evaluation
    User selects a module or function (e.g., Inventory, HR, Finance)
    System checks:
        Is requested operation permitted for user's role?
            If Yes: Grant access
            If No: Deny access, log violation
4 Module Execution

If access granted:
Load requested ERP module #Defined functions (financial management, inventory management, sales management, project management, supply chain management)
Allow permitted actions (e.g., view, edit, delete)
Log activity in AuditTrail

5 Security Monitoring
Run periodic checks for:
Role conflicts (e.g., Segregation of Duties (SoD) violations) #happens when a user has access or permissions that allow them to perform conflicting tasks.
Suspicious behaviour (access outside work hours)
Trigger alerts if anomaly is detected

6 Session Termination
On logout or timeout:
Save session log
Close database connection
Display "Logout Successful"

7 End System

The proposed system presented in Algorithm 1 outlines a secure and efficient workflow for an ERP system integrated with RBAC which begins with user authentication, where credentials are verified against a secure database. Upon successful login, the system identifies the user's role and loads corresponding permissions. When a user requests access to a module such as Finance, HR, or Inventory data, the system evaluates whether their role permits the requested operation and if authorized, access is granted and the user's actions are logged for audit purposes; otherwise, access is denied and the attempt is recorded. The algorithm presented incorporates continuous security monitoring to detect conflicts in roles or suspicious behaviour, such as unauthorized access attempts or activity outside normal working hours. This structured approach ensures that users can only access the functions relevant to their roles, enhancing both system security and operational efficiency. Algorithm 2 presents the structural stepwise implementation for RBAC definition and implementation.

Algorithm 2: RBAC Definition Algorithm
// Define access levels for different user roles
// Higher number = higher privileges
1. DEFINE Access Levels = {
2. "Admin": 4, //Full access to all ERP modules and configurations
3. "Manager": 3, //Can manage teams, approve tasks, view reports
4. "Staff": 2, //Can update records, perform assigned operations
5. "Viewer": 1 //Read-only access, no modification rights
}
//Function to get the numerical access level of a user based on their role
6. FUNCTION get User Access Level (user): //Get access level from input of the user
//Compare the input to ascertain the access permission of the user from the Database
7. RETURN Access Levels [user.role]
//Function to determine if the user is authorized to perform a specific task
//Compares the user's level with the minimum required level
8. FUNCTION is Authorized (user, required Level):
9. User Level = get User Access Level(user)
10. IF user Level >= required Level THEN
//If the user has sufficient privileges
11. RETURN True
12. ELSE //If the user's level is too low
13. RETURN False

This algorithm performs the logic for user access authorization by the RBAC technique in the ERP Module of the proposed intelligent system. The integration of the Algorithm 2 into the intelligent ERP system for access level RBAC system, Algorithm 3 is produced which demonstrates the implementation of the RBAC integrated into the ERP

Algorithm 3: RBAC integrated into ERP Module
// Implement login input
INPUT username = "sylvia"
INPUT password = " 1234567890"
// Attempt login
Authenticated User = login (username, password)
IF authenticated User IS NOT null THEN
PRINT "Login Successful. Role: " + authenticated User. role

© FEB 2026 | IRE Journals | Volume 9 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I8-1714299

// Define task requirements

Required Level = Access Levels ["Manager"] // Task needs Manager or higher

// Check permission

IF is Authorized (authenticated User, required Level) THEN

PRINT "Access Granted: You may perform this task."

ELSE

PRINT "Access Denied: Your role does not permit this action."

ELSE

PRINT "Login Failed: Invalid credentials."

3.2 System Flowchart

This section presents the diagrammatic flow of the algorithm which reports the sequencies series of steps and decisions made in the system throughout the operational steps. The flowchart of the proposed intelligent ERP system for this study is shown in Figure 1, where RBAC technique is used to grant access to users of the platform.

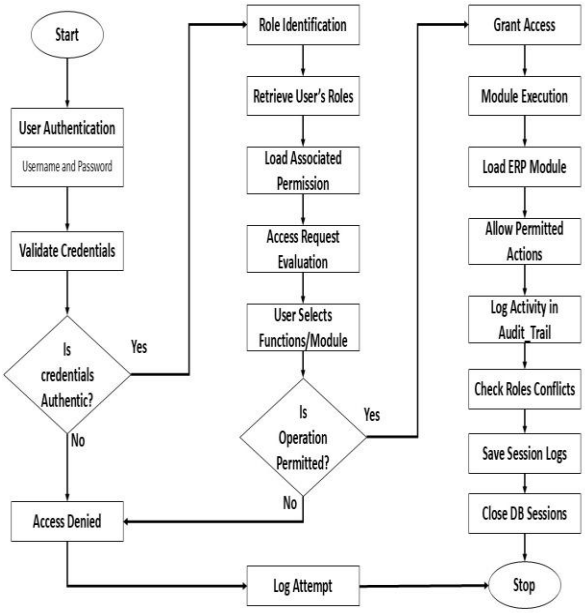

Figure 1: System Flowchart

Figure 1 offers a clear and structured view of how Intelligent RBAC operates within an ERP system. It walks through the user journey from logging in and verifying credentials, to identifying roles and checking permissions for requested actions. If access is approved, the system loads the relevant module and tracks user activity for accountability. Alongside this, it continuously monitors for suspicious behaviour or role conflicts, ensuring security remains tight throughout the session. When the user logs out or times out, the system wraps up by saving logs and closing connections. Overall, the flowchart highlights how smart access control and real-time oversight work together to keep the ERP system secure and efficient. Figure 2 presents the flowchart of the RBAC access level implementation.

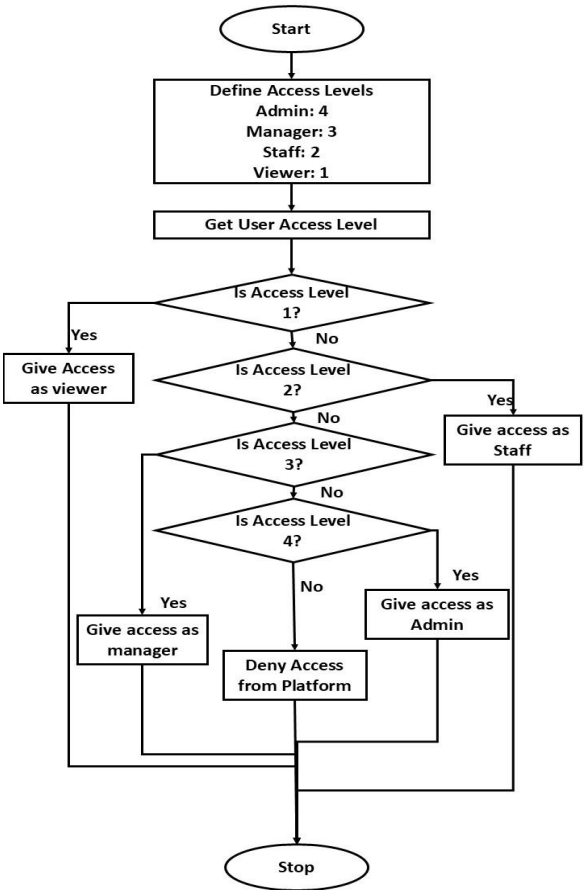

Figure 2: Flowchart of the RBAC Based ERP Module

Figure 2 lays out the logic of user access control in a straightforward, easy-to-follow flowchart. At its core, it shows how the system determines a user's privileges by matching their access level ranging from Viewer (1) to Admin (4) with the corresponding set of permissions. As the system retrieves this access level, it compares it against a clear, predefined hierarchy to decide what the user is allowed to do. For instance, a Viewer may only see content, while a manager can oversee operations and an Admin holds

© FEB 2026 | IRE Journals | Volume 9 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I8-1714299

full control. This organized structure makes it simple for the ERP system to assign and manage roles efficiently, striking the right balance between usability and security. Figure 3 represent the flowchart of the integrated ERP system with RBAC technique for a controlled user access

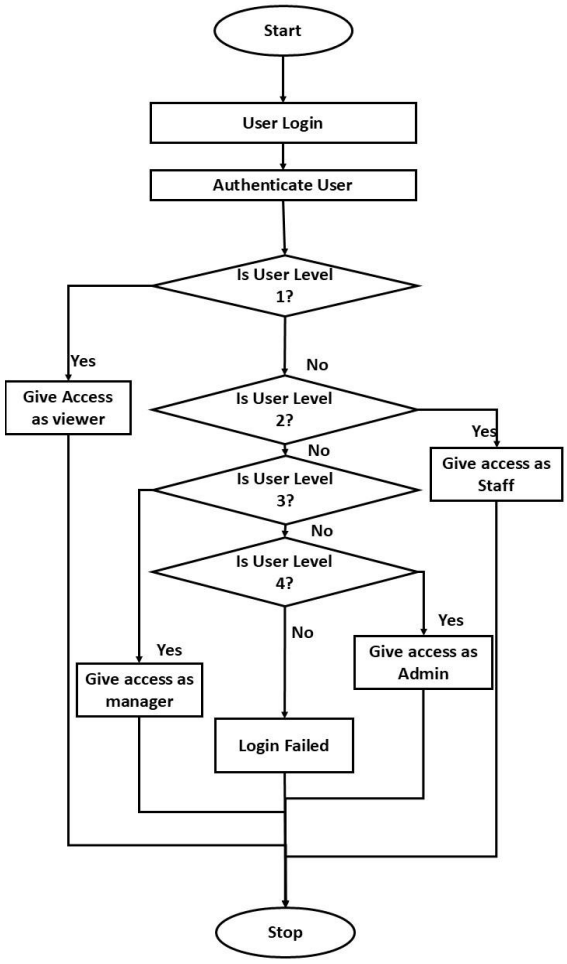

Figure 3: Flowchart of the ERP-RBAC system

Figure 3 reports the functional integration flowchart of the proposed intelligent ERP-RBAC system. The flowchart demonstrates the flow of user access from login for accessing the authentication level of the user in order to determine the access the user gets on the platform.

IV. SYSTEM SOFTWARE TESTING

This section presents the system testing which is a set of activities that can be planned in advance and conducted systematically. The testing presented in this section demonstrates the implementation phases of the proposed intelligent system developed as a web-based application. This chapter handles every form of testing necessary to evaluate the system performance. Figure 4 presents the login interface of the intelligent ERP system

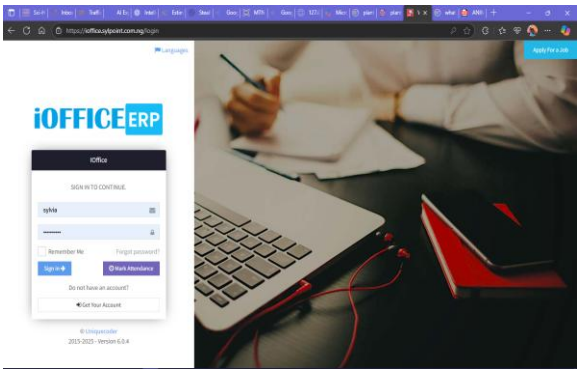

Figure 4: Login Page

Figure 4 presents a structured and intuitive user interface for accessing the intelligent ERP system. The layout balances functionality with professional aesthetics: the left section features essential input fields for username and password, along with links for account recovery and registration. These components ensure secure and efficient access for users while supporting routine workflows. Together, the design emphasizes usability, security, and a work-centric identity, making it well-suited for office professionals seeking a reliable entry point into the ERP system.

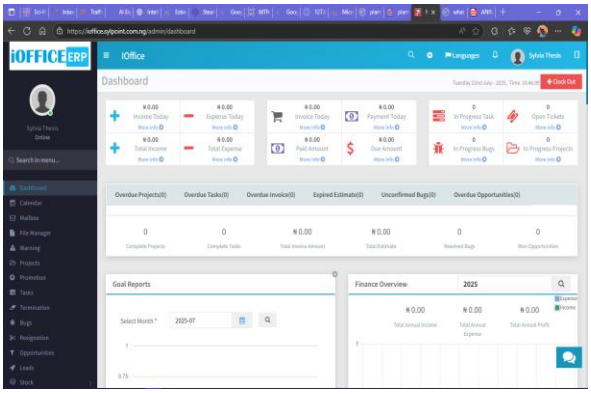

Figure 5: System Dashboard

Figure 5 showcases the interactive dashboard of the intelligent ERP system, which serves as the hub for users to access real-time business operations on the platform. The interface is thoughtfully laid out with

© FEB 2026 | IRE Journals | Volume 9 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I8-1714299

metric cards for tracking income, expenses, invoices, payments, tasks, projects, bugs, and tickets giving users a summary of operational performance. Additionally, progress indicators and charts highlight yearly financial goals and goal reports for various years which promotes data-driven decision-making. This dashboard merges depth with usability, enabling stakeholders/users the opportunity to monitor workflows and manage resources efficiently in a streamlined workspace. Figure 6 presents the page for the user/admin to manage stocks from the stock lists available

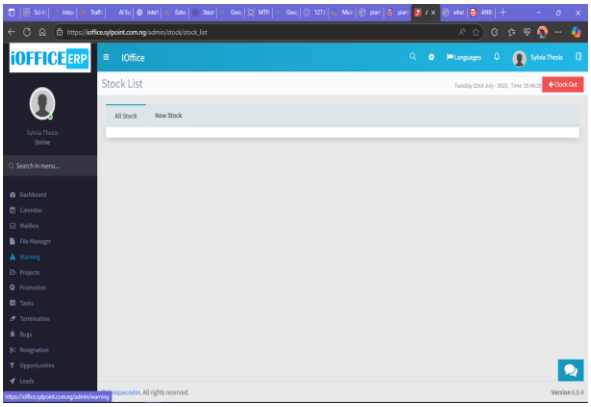

Figure 6: Stock List Layout

The image in Figure 6 presents the inventory management interface of the intelligent system which provides a streamlined environment for stock tracking and categorization. Dominated by a clean design, the layout features a header titled "Stock List" alongside navigation tabs labelled "All Stock" and "New Stock," making it easy for users to toggle between inventory views. This layout promotes usability and clarity, enabling seamless inventory operations within broader business workflows. Figure 7 illustrates the user's management layout of the system.

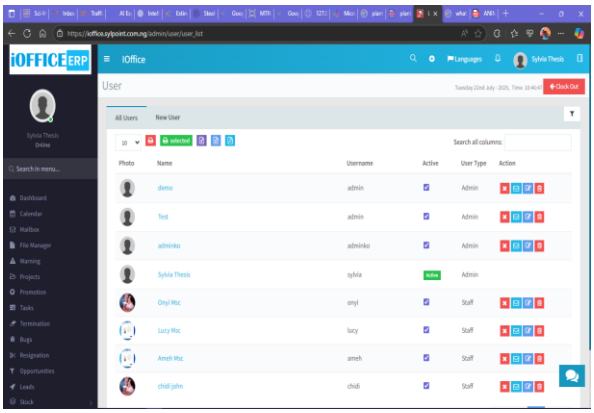

Figure 7: User Access Level Definition Page

Figure 7 presents the User Management interface of the intelligent system, offering administrators a structured and intuitive platform to oversee user accounts. The layout features a dynamic table with user attributes such as profile photo, full name, username, active status, assigned user role (Admin or Staff), and actionable icons for editing, viewing or deleting each user or admin profile. This design ensures streamlined control over access permissions and user engagement across the ERP environment supporting secure role-based access and real-time account management.

V. CONCLUSION

This study set out to improve the security and operational efficiency of intelligent ERP systems by integrating a RBAC mechanism tailored for office data control and management. By reading the literature carefully, it was identified that there was gap in researches where most ERP systems have integrated features of artificial intelligence and other advanced operations but they lack well-established structures of access control especially in the case of SMEs and in less-developed economies. In order to cope with it, an RBAC algorithm was developed to provide and impose user roles, access privileges, and restrictions to access, so that the users can work with the ERP platform in a controlled and responsible way.

The system was further implemented as a user-friendly software application that demonstrates the practicality of RBAC in real-world ERP environments. Testing and validation through user

feedback confirmed that the system not only enhances data security but also improves usability and administrative control over business processes. This research thus contributes a valuable solution to ERP security challenges, combining theoretical innovation with practical implementation. Finally, the study underscores the importance of integrating intelligent access control mechanisms into ERP systems to support secure, scalable, and efficient office operations. The proposed RBAC-enhanced ERP framework holds significant promise for broader adoption across diverse organizational contexts, especially where data sensitivity and operational integrity are paramount.

REFERENCES

[1] Accenture. (2020). 2020 ERP trends: Turning intelligence into value. https://www.accenture.com/_acnmedia/PDF-119/Accenture-ERP-Report-2020.pdf

[2] Brodzik, C., Lamar, K., & Shaikh, A. (2020). Tech trends 2021. Deloitte Insights. https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021 Tech-Trends.pdf

[3] Clark, K. (2022, May 19). Yahoo lawsuit alleges employee stole trade secrets upon receiving Trade Desk job offer. The Drum. https://www.thedrum.com/news/2022/05/19/yahoo-lawsuit-alleges-employee-stole-trade-secrets-upon-receiving-trade-desk-job

[4] Gaikwad, V., & Rachita, R. (2021). Enterprise resource planning (ERP) market by component: Global opportunity analysis and industry forecast, 2019–2027. Allied Market Research. https://www.alliedmarketresearch.com/erp-market

[5] Gessa, A., Jiménez, A., & Sancha, P. (2023). Exploring ERP systems adoption in challenging times: Insights of SMEs stories. Technological Forecasting and Social Change, 195, Article 122795. https://doi.org/10.1016/j.techfore.2023.122795

[6] Goldston, J. (2020). The evolution of ERP systems: A literature review. International Journal of Research, 50, 1–18.

[7] Malik, A. K., Emmanuel, N., Zafar, S., Khattak, H. A., Raza, B., Khan, S., Al-Bayatti, A. H., Alassafi, M. O., Alfakeeh, A. S., & Alqarni, M. A. (2020). From conventional to state-of-the-art IoT access control models. Electronics, 9(10), Article 1693. https://doi.org/10.3390/electronics9101693

[8] Marquis, Y. A. (2024). From theory to practice: Implementing effective role-based access control strategies to mitigate insider risks in diverse organizational contexts. Journal of Engineering Research and Reports, 26(5), 138–154. https://doi.org/10.9734/JERR/2024/v26i51141

[9] Paganini, P. (2022, April 6). Block discloses data breach involving Cash App potentially impacting 8.2 million US customers. Security Affairs. https://securityaffairs.com/129892/data-breach/block-cash-app-data-breach.html

[10] Rashid, A. B., & Kausik, M. A. K. (2024). AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications. Hybrid Advances, 7, Article 100277. https://doi.org/10.1016/j.hybadv.2024.100277

[11] Taherdoost, H. (2022). The role of different types of management information system applications in business development: Concepts, and limitations. Cloud Computing and Data Science. https://doi.org/10.37256/ccds.4120231959

[12] Uemerson, A. de C. S. (2020). Intelligent ERPS: A guide to incorporate AI into enterprise resource planning systems [Master's thesis or dissertation]. Universidade Nova de Lisboa.

[13] William, F., & Tjhin, V. U. (2021). The evaluation of enterprise resource planning application using information systems success model. Journal of Management Information and Decision Sciences, 24(5), 1–13.